a' cont

member, separating by the second member the second session key from the key exchange response message if the second member is a participating member, separating by the second member the first session key for each of the first members from the key exchange response message, and sending each of the first session keys to its respective first member.

In the Claims:

Please cancel claims 1-53 without prejudice.

Please add the following new claims:

a2

54. (New) A method of conducting an electronic transaction using an electronic card having a public key of a service provider, the method comprising:

initiating a transaction at a cardholder location by encrypting at least a portion of a message with the service provider's public key from the electronic card and sending the message to a service provider location; and

completing the transaction between the cardholder and the service provider in response to the message.

55. (New) The method of claim 54 wherein the message comprises a key exchange request message, the initiation of the transaction further comprising:

generating a session key at the service provider location in response to the key exchange request message;

formatting a key exchange response message having the session key at the service provider location; and

sending the key exchange response message to the cardholder location; wherein the transaction is completed using the session key.

56. (New) The method of claim 55 wherein the key exchange request message includes a public key of the of the cardholder

57. (New) The method of claim 54 wherein the message comprises a key exchange request message having a public key of the cardholder and a cardholder challenge for the service provider, the initiation of the transaction further comprising;

generating a session key at the service provider location in response to the key exchange request message;

formatting a key exchange response message at the service provider location comprising the session key, a response for the cardholder challenge and a service provider challenge for the cardholder;

sending the key exchange response message to the cardholder location; and

formatting a response for the service provider challenge at the cardholder location and sending it to the service provider location;

wherein the transaction is completed using the session key.

58. (New) The method of claim 56 or 57 wherein the initiation of the transaction further comprises:

formatting a transaction request message using the session key at the cardholder location;

digitally signing the transaction request message at the cardholder location;

sending the transaction request message from the cardholder location to the service provider location;

formatting, at the service provider location, a transaction response message for the cardholder using the session key;

digitally signing the transaction response message at the service provider location; and

sending the transaction response message to the cardholder location.

59. (New) The method of claim 58 wherein the transaction request message includes account information, transaction amount, and transaction data each being encrypted with the session key.

60. (New) The method of claim 58 wherein the transaction request message includes plain text.

61. (New) The method of claim 58 wherein the transaction request message includes a transaction identifier assigned to the cardholder by the service provider.

62. (New) The method of claim 58 wherein the transaction response message includes plain text.

63. (New) The method of claim 58 wherein the transaction response message includes a transaction identifier assigned to the cardholder by the service provider.

64. (New) The method of claim 58 wherein the initiation of the transaction further comprises:

formatting, at the cardholder location, a transaction acknowledgment message using the session key;

digitally signing the transaction acknowledgement message at the cardholder location; and

sending the transaction acknowledgment message to the service provider location.

65. (New) The method of claim 64 wherein transactional acknowledgement message comprises acknowledgement data encrypted with the session key.

66. (New) The method of claim 64 wherein the transactional acknowledgement message comprises plain text.

67. (New) The method of claim 64 wherein the transactional acknowledgement message comprises a transaction identifier assigned to the cardholder by the service provider.

68. (New) The method of claim 54 wherein the message comprises a key exchange request comprising a public key of the cardholder and a first cryptogram having a cardholder challenge encrypted with the service provider's public key from the electronic card, the initiation of the transaction further comprising:

digitally signing the key exchange request message at the cardholder location;

sending the key exchange request message from the cardholder location to the service provider location;

generating a second cryptogram at the service provider location in response to the key exchange request message, the second cryptogram comprising a service provider challenge and a session key together encrypted with the cardholder's public key;

formatting, at the service provider location, a key exchange response message including the second cryptogram and a response to cardholder challenge;

digitally signing the key exchange response message at the service provider location;

sending the key exchange response message from the service provider location to the cardholder location;

generating, at the cardholder location, a third cryptogram comprising a service provider challenge response encrypted with the session key;

attaching the third cryptogram to a transaction message; and

digitally signing both of the transaction message and the third cryptogram together at the cardholder location, and sending them to the service provider location.

69. (New) The method of claim 68 wherein the key exchange request message and key exchange response message each comprises plain text.

70. (New) The method of claim 68 wherein the key exchange request message comprises the cardholder's public key encrypted with the service provider's public key.

71. (New) The method of claim 68 wherein the generation of the second cryptogram further comprises encrypting a cardholder challenge response as part of the second cryptogram.

72. (New) The method of claim 68 wherein the generation of the second cryptogram further comprises encrypting a transaction identifier as part of the second cryptogram.

73. (New) The method of claim 68 wherein the key exchange response message further includes a transaction identifier comprising plain text.

74. (New) The method of claim 73 further comprising using the transaction identifier with a second transaction message following the transaction message and going from the cardholder location to the service provider location.

75. (New) The method of claim 54 wherein the message comprises a key exchange request message having a public key of the cardholder, and wherein the sending of the key exchange request message comprises sending the key exchange request message from the cardholder location to a second cardholder location and from a second cardholder location to the service provider location, the initiation of the transaction further comprising:

combining, at the second cardholder location, the key exchange request message from the cardholder location with a second key exchange request message generated at the second cardholder location, and sending the combined key exchange request message, signed at the second cardholder location, to the service provider location;

formatting a key exchange response message at the service provider location including a session key for the cardholder location and digitally signing the key exchange response message, formatting a key exchange response message including a second session key for the second cardholder location, combining the key exchange response messages into a combined key exchange response message, signing the

combined key exchange response message at the service provider location, and sending the combined key exchange response message from the service provider location to the second cardholder location; and

separating, at the second cardholder location, the key exchange response messages for the second cardholder location from the key exchange response message for the cardholder location, and forwarding the key exchange response message for the cardholder location to the cardholder location.

76. (New) The method of claim 75 further comprising:

formatting, at the first cardholder location, a transaction request message using the session key for the cardholder location and digitally signing the transaction request message;

sending the transaction request message from the cardholder location to the second cardholder location;

formatting, at the second cardholder location, a transaction request message using the session key for the second cardholder location;

combining, at the second cardholder location, the transaction request messages into a combined transaction request message and digitally signing the combined transaction request message;

sending the combined transaction request message from the second cardholder location to the service provider location;

formatting, at the service provider location, a transaction response message using the session key for the cardholder location and digitally signing the transaction response message;

formatting, at the service provider location, a transaction response message using the session key for the second cardholder location;

combining the transaction response messages into a combined transaction response message and digitally signing the combined transaction response message at the service provider location;

sending the combined transaction response message to the second cardholder location;

separating, at the second cardholder location, the transaction response message into the transaction response message for the cardholder location and the transaction response message for the second cardholder location; and

forwarding the transaction response message for the cardholder location from the second cardholder location to the cardholder location.

77. (New) The method of claim 76 further comprising:

formatting, at the cardholder location, an acknowledgment message using the session key for the cardholder location and digitally signing the acknowledgement message;

sending the acknowledgment message from the first cardholder location to the second cardholder location; and

formatting, at the second cardholder location, an acknowledgment message using the session key for the second cardholder location, combining the acknowledgment messages into a combined acknowledgment message, and digitally signing the combined acknowledgement message at the second cardholder location; and

sending the combined acknowledgment message from the second cardholder location to the service provider location.

78. (New) The method of claim 77 wherein the session keys are the same.

79. (New) The method of claim 77 wherein the session keys are different.

80. (New) The method of claim 77 wherein the key exchange response message for the second service provider member terminal includes the public key for the service provider member terminal, and the key exchange response message for the cardholder location includes a public key of the second cardholder location.

81. (New) A method of conducting an electronic transaction using an electronic card having a public key of a service provider, comprising:

formatting a key exchange request message at a member, at least a portion of the key exchange request message being encrypted using the service provider's public key from the electronic card;

sending the key exchange request message from the member to the service provider;

generating a session key at the service provider in response to the key exchange request message;

formatting a key exchange response message including the session key at the service provider;

sending the key exchange response message from the service provider to the member; and

using the session key to complete the transaction.

82. (New) The method of claim 81 wherein the key exchange request message includes a public key of the member.

83. (New) The method of claim 82 wherein the key exchange request message further includes a member challenge for the service provider, and the key exchange response message further includes a response to the member challenge and a service provider challenge for the member, the method further comprising formatting by the member a response to the service provider challenge and sending it to the service provider.

84. (New) The method of claim 82 or 83 wherein the use of using the session key to complete the transaction comprises:

formatting by the member a transaction request message using the session key, the transaction request message including a digital signature of the member, and sending the transaction request message to the service provider; and

formatting at the service provider, a transaction response message for the member using the session key, the transaction response including a digital signature of the service provider, and sending the transaction response message to the member.

85. (New) The method of claim 84 wherein the transaction request message includes account information, transaction amount and transaction data, and wherein the formatting of the transaction request message by the member comprises encrypting with the session key the account information, the transaction amount and a portion of the transaction data.

86. (New) The method of claim 84 wherein the transaction request message comprises plain text.

87. (New) The method of claim 84 wherein the transaction request message comprises a transaction identification assigned to the member by the service provider.

88. (New) The method of claim 84 wherein the transaction request message comprises the response to a service provider challenge.

89. (New) The method of claim 84 wherein the transaction response message includes data encrypted with the session key a portion of the data.

90. (New) The method of claim 84 wherein the transaction response message includes plain text.

91. (New) The method of claim 84 wherein the transaction response message includes a transaction identifier assigned by the service provider to the member.

92. (New) The method of claim 84 further comprising formatting at the member, using the session key, a transaction acknowledgment message, digitally signing by the member the transaction acknowledgment message, and sending the transaction acknowledgment message to the service provider.

93. (New) The method of claim 92 wherein the transaction acknowledgement message includes data encrypted with the session key.

94. (New) The method of claim 92 wherein the transaction acknowledgement message includes plain text.

95. (New) The method of claim 92 wherein the transaction acknowledgement message includes a transaction identifier assigned to the member by the service provider.

96. (New) A method of conducting an electronic transaction using an electronic card having a public key of a service provider, comprising:

generating a member challenge by the member;

encrypting by the member the member challenge using the service provider's public key from the electronic card to generate a first cryptogram;

formatting by the member a key exchange request message including the first cryptogram and a public key of the member;

signing digitally by the member the key exchange request message;

sending the digitally signed key exchange request message to the service provider;

generating by the service provider a service provider challenge;

generating by the service provider a session key;

encrypting by the service provider the service provider challenge and the session key using the member's public key to generate a second cryptogram;

formatting by the service provider a key exchange response message including the second cryptogram and a response to member challenge;

signing digitally by the service provider the key exchange response message;

sending the digitally signed key exchange response message to the member;

encrypting by the member a member response for the service provider challenge using the session key to generate a third cryptogram;

attaching the third cryptogram to a transaction message going from the member to the service provider;

signing digitally by the member the transaction message going from the member to the service provider; and

sending the transaction message going from the member to the service provider to the service provider.

97. (New) The method of claim 96 wherein the key exchange request message and key exchange response message each comprises plain text.

98. (New) The method of claim 96 wherein the key exchange request message comprises the cardholder's public key encrypted with the service provider's public key.

99. (New) The method of claim 96 wherein the generation of the second cryptogram further comprises encrypting a cardholder challenge response as part of the second cryptogram.

100. (New) The method of claim 96 wherein the generation of the second cryptogram further comprises encrypting a transaction identifier as part of the second cryptogram.

101. (New) The method of claim 96 wherein the key exchange response message further includes a transaction identifier comprising plain text.

102. (New) The method of claim 101 further comprising using the transaction identifier with a second transaction message following the transaction message and going from the cardholder location to the service provider location.

103. (New) A method of communication using an electronic card having a public key of a service provider, comprising:

formatting a first key exchange request message at a first member, the first key exchange request message having a public key of the first member, and at least a portion of the first key exchange request message being encrypted using the service provider's public key from the electronic card;

sending the first key exchange request message from the first member to a second member;

combining at a second member, a second member key exchange request message with the first member's key exchange request message and sending the combined key exchange request message, signed by the second member, to a service provider;

formatting a key exchange response message at the service provider including a first session key for the first member, signing the response message, formatting a key exchange response message including a second session key for the second member, combining the key exchange response messages into a combined key exchange response message, signing the combined key exchange response message, and sending the combined key exchange response message to the second member; and

separating at the second member, the key exchange response message for the second member from the key exchange response message for the first member, and forwarding the key exchange response message for the first member to the first member.

104. (New) The method of claim 103 further comprising:

formatting by the first member, using the first session key, a transaction request message, signing the transaction request message, and sending the transaction request message to the second member;

formatting by the second member, using the second session key, a transaction request message;

combining by the second member, the second member transaction request message with the first member transaction request message, signing the combined transaction request message, and sending the combined transaction request message to the service provider;

formatting by the service provider, using the first session key, a transaction response message for the first member, and signing the transaction response message;

formatting by the service provider, using the second session key, a transaction response message for the second member;

combining the transaction response message for the first member with the transaction response message for the second member to form a combined transaction response message, and signing the combined transaction response message;

sending the combined transaction response message to the second member;

a2 cont

separating at the second member, the transaction response message for the first member from the transaction response message for the second member; and

forwarding by the second member the transaction response message for the first member to the first member.

105. (New) The method of claim 104 further comprising:

formatting at the first member, using the first session key, an acknowledgment message, signing the acknowledgment message, and sending the acknowledgment message to a second member; and

formatting at the second member, using the second session key, an acknowledgment message, combining the second member acknowledgment message with the first member acknowledgment message to form a combined acknowledgment message, signing the combined acknowledgment message, and sending the combined acknowledgment message to the service provider.

106. (New) The method of claim 103 wherein the first session key is different from the second session key.

107. (New) The method of claim 103 wherein the first session key is the same as the second session key.

108. (New) The method of claim 103 wherein the key exchange response message for the second member includes the public key of the first member, and the key exchange response message for the first member includes the public key of the second member.

109. (New) A method of communication using an electronic card having a public key of a service provider, comprising:

formatting a first key exchange request message at a first member, the first key exchange request message having a public key of the first member, and at least a portion of the first key exchange request message being encrypted using the service provider's public key from the electronic card;

sending the first key exchange request message from the first member to at least one intermediate member coupled in series between the first member and the service provider, each of said at least one intermediate member being either a message router or a participating member;

generating, if said at least one intermediate member comprises at least one participating member, at each of the participating members a key exchange request;

receiving at the service provider a combined key exchange request message from said at least one intermediate member, the combined key exchange request message comprising the first key exchange request message and the key exchange request message generated by each of the participating members;

generating at the service provider a first session key for the first member and a participating session key for each of the participating members;

formatting at the service provider a key exchange response message including each of the first and participating session keys;

sending the key exchange response message from the service provider to said at least one intermediate member;

separating by each participating member its respective participating session key from the key exchange response message; and

sending the first session key from said at least one intermediate member to the first member.

110. The method of claim 109 further comprising:

encrypting a first transaction request message using the first session key at the first member;

sending the first transaction request message from the first member to said at least one intermediate member;

generating, if said at least one intermediate member comprises at least one participating member, at each of the participating members a transaction request message encrypted using its respective participating session key;

receiving at the service provider a combined transaction request message from said at least one intermediate member, the combined transaction request message comprising the first transaction request message and the transaction request message for each of the participating members;

formatting at the service provider a combined transaction response message comprising a transaction response message for the first member and each of the participating members;

sending the combined transaction response message from the service provider to said at least one intermediate member;

separating by each participating member its respective transaction response message from the combined transaction response message; and

sending the transaction response message for the first member from said at least one intermediate member to the first member.

111. (New) The method of claim 109 wherein the first session key and the participating session keys are each different from one another.

112. (New) The method of claim 109 wherein the first session key and the participating session keys are the same as each other.

113. (New) A method of communication using an electronic card having a public key of a service provider, comprising:

formatting a key exchange request message at each of a plurality of first members, the key exchange request message for one of the first members having a public key of said one of the first members, and at least a portion of the key exchange request message for said one of the first members being encrypted using the service provider's public key from the electronic card;

sending from each of the first members its respective key exchange request message to a second member, the second member being either a message router or a participating member;

generating, if the second member is a participating member, a second key exchange request message at the second member;

combining at the second member the key exchange request message from each of the first members to form a combined key exchange request message, the combined key exchange request message further comprising the second key exchange request message if the second member is a participating member;

receiving at the service provider the combined key exchange request message from the second member;

generating at the service provider a first session key for each of the first members, and a second session key for the second member if the second member is a participating member;

formatting at the service provider a key exchange response message including each of the first and second session keys;

sending the key exchange response message from the service provider to the second member;

separating by the second member the second session key from the key exchange response message if the second member is a participating member;

separating by the second member the first session key for each of the first members from the key exchange response message; and

sending each of the first session keys to its respective first member.

114. (New) The method of claim 113 further comprising:

encrypting a transaction request message at each of the first members using their respective first session keys;

sending from each of the first members its respective transaction request message to the second member;

generating, if the second member is a participating member, a second transaction request message at the second member and encrypting the second transaction request message with the second session key;

combining at the second member the transaction request message from each of the first members to form a combined transaction request message, the combined transaction request message further comprising the second transaction request message if the second member is a participating member;

A2 cont

receiving at the service provider the combined transaction request message from the second member;

generating at the service provider a transaction response message for each of the first members, and the second member if the second member is a participating member;

formatting at the service provider a combined transaction response message including the transaction response messages for each of the first members, and the second member if the second member is a participating member;

sending the combined transaction response message from the service provider to the second member;

separating by the second member its respective transaction response message from the combined transaction response message if the second member is a participating member;

separating by the second member the transaction response messages for each of the first members from the combined transaction response message; and

sending each of the transaction response messages to its respective first member.

115. (New) The method of claim 113 wherein the first session keys and the second session key are each different from one another.